REMARKS

In response to the Official Action dated 5/12/2008, the above-identified application has been amended to place the claims in better condition for allowance. Review and reconsideration are requested in view of the above amendments and following remarks.

In the Office Action of 5/12/2008, the Examiner states as follows:

> **Claims 1 – 8 and 10 – 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aziz et al. (Aziz), "Method and Apparatus for Providing Secure Communication with a Relay in a Network", U.S. Patent 6,643,701 in view of Gast, "System and Method for Accelerating Cryptographically Secured Transactions", U.S. Patent Publication 2003/0046532.**

In the most recent Office Action, the Examiner relies on Aziz, FIG. 3 as teaching multiple SSL connections between the same client and server. Applicants have taken note of Examiner's comments and amended the application accordingly.

In reading Aziz, Aziz provides for a session resumption procedure for handling a break in an existing SSL communication link. Aziz points this out as seen in Column 8, lines 42-65, which states:

> After the handshaking session is completed, the secure connection program of client 300 and the secure connection program of relay 320 create a link 310 between client 300 and relay 320. The secure connection program of client 300 initiates transfer of information from client 300 to the secure connection program of server 340 over link 310, through relay 320, and over link 330. *Because link 330 may have been idle for sometime, link 330 may be broken in this case, the secure connection program of relay 320 and the secure connection program of server 340 must reestablish link 330 using a session resumption procedure (step 950).* In this case, the secure connection program of relay 320 simply identifies itself to server 340 and indicates that it will continue to use the agreed upon keys from the previous handshaking session. Secure connection program of

> server 340 would acknowledge that the end-to-end security session should be resumed and create link 330. Once links 310 and 330 are established, the secure connection program of client 300 and the secure connection program of server 340 transfer information between client 300 and server 340 through relay 320. Then data processing program in relay 320 can then intercept the transferred information and reformat or test the information, in a manner consistent with advantages of the present invention (step 960).

Accordingly, Aziz does not teach, disclose or suggest Applicants' claimed invention which provides for concurrent secure connections between the same server and client. Aziz does not alone or in combination with any of the cited references teach, disclose or suggest the claimed invention. Aziz is directed to a method and apparatus for providing secure communication with a relay in a network. Converse to the examiner's position, Aziz teaches away from the present invention. Col. 6, lines34-48 state"

> In FIG. 3, a server 340 provides intermediate relays 320 with information that can authenticate the relays as server 340. Each client 300 negotiates an end-to-end secure transmission link 310 with a particular relay 320. Each relay is connected to a server through another end-to-end secure transmission link 330 to server 340. This structure allows secure transmission of information from the client 300 to server 340.
>
> If the network between relays 320 and server 340 is trusted (as would be the case if the relays, network, and server were all in the same facility) and therefore secure, connection 330 could even be cleartext HTTP connection, reducing the server workload even more compared to using previously negotiated SSL sessions, as will be discussed below.

It is clear that Aziz only discloses making a single connection between each client and a relay and a relay and a server at any one given time. Moreover, Aziz states that the connection can be a cleartext HTTP connection. This can be a problem and create a security issue because Basic credentials are Base64-encoded. If Basic credentials are sent over an HTTP connection, they may be read as clear text and decoded.

Column 6, lines 4-24 simply indicate that there could be multiple clients, relays or servers. However, in the cases disclosed each paradigm fails to show multiple concurrent SSL connections between the same client and server. Rather, there is simply shown the inclusion of the means to create a single secure connection between the client/relay and relay/server or refresh/resume a connection.

There is no disclosure, suggestion or teaching in Aziz as to the need or means how to make multiple concurrent SSL connections with the same client and same server. This is only taught by the present invention.

Gast is directed to a system and method for accelerating cryptographically secured transactions. Gast is concerned with offloading encryption processing to central encryption servers equipped with hardware built to accelerate encryption speed and reduce latency [paragraph 0015]. Gast simply moves the task of processing the security mechanism, i.e., establishing a SSL session to a central control point [0022]. The point stressed in Gast is to offload the establishment of SSL connections by the server, not to establish additional concurrent SSL connections between the client and server as opposed to the instant invention which provides a CA certificate and a pseudo CA certificate to establish concurrent SSL connections through whereby data can pass in a compressed form, for example, in the second established connection. Gast teaches away from the instant invention.

Likewise as stated above, Aziz attempts leads toward offloading the SSL connection by using a cleartext HTTP connection, i.e., Aziz states "reducing the server workload even more compared to using previously negotiated SSL sessions". In any case, combining the references in no way would result in the present claimed invention and in fairly interpreting the teachings of each and combining such teachings a reasonable combination at best would be the combination of offloading encryption processing further with the aid of relays. This does not render the instant invention. Withdrawal of the rejection of claims under 35 U.S.C. over Aziz in view of Gast is respectfully requested.

The Examiner stated:

> **Claims 9 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Aziz and Gast in view of Freed et al. (Freed), "Secure Sockets Layer Proxy Architecture", U.S. Patent Publication 2003/0014628.**

In view of the above amendments and remarks, this is also traversed. Freed et al. discloses a secure sockets layer architecture which employs an intermediate device between the client computer and the server computer which intercepts SSL/TCP data and then performs one or more transactions to aid in acceleration. Like Aziz, there is no direct link between the client computer and the server computer. As seen in paragraphs [0007-0010] of Freed et al., there is merely a conventional SSL handshake which is employed and all secure data is sent through the one secure tunnel which is created. Freed et al are concerned with offloading the server the task of encryption/decryption task by employing a tertiary or intermediary device to interact with the client and the server. Nevertheless, the tertiary computer employs conventional handshake technology.

This is very different from the instant invention. The present invention calls for a system for increasing data access in a secure socket layer network environment, which includes:

a web server computer having SSL protocol server software operably associated therewith for enabling a SSL connection, wherein SSL protocol server software includes a CA certificate and private key, SSL acceleration server software operably associated with the web server computer which includes a pseudo CA certificate and access to the private key and a public key; and

a client computer communicatively linked to the web server computer having web browser software having SSL protocol client software operably associated therewith for enabling a first SSL connection between the client and the web server, SSL acceleration client software operably associated with the client computer which communicates with the SSL acceleration server software to receive a copy of the pseudo CA certificate and the public key and present the pseudo CA certificate to the web browser software for validation thereof for enabling a second concurrent SSL connection between the client computer and the web server computer in a manner which permits optimization techniques to be applied on data transmitted through said second SSL connection. The invention also claims one of direct and indirect connection between the same client/server. A method employing these elements is also provided.

The instant invention provides a server with SSL protocol server software and SSL acceleration server software on both the client and server for enabling direct and concurrent multiple SSL sessions to take place through the use of creating a pseudo CA certificate on the web server in addition to having the existing CA certificate on the web server which are presented to the client computer having SSL protocol and SSL acceleration software thereon. By so providing, multiple direct secure links are created. Freed et al., like Aziz, introduces a third element in the chain of connection and another potential break point for communication.

The instant invention enables secure data be transacted using the CA certificate from the web server over an initial SSL connection for transacting key data which must pass over such connection, such as when connecting to a secure bank site, for example. In addition, the instant invention provides the pseudo CA certificate and secondary concurrent SSL connection through which data may pass in a secure connection which enables functional operations (optimization techniques) to be performed thereon, such as compression of data. This is not taught, disclosed or suggested in Freed et al. (or Aziz) and this can't be accomplished in the teachings of Freed et al or Aziz. Freed et al. only acts as an intermediary intercepting all communication over the existing SSL connection and passes the data accordingly, paragraph [0039]. Paragraphs [0052] - [0053] and the claims in Freed et al. further illustrate Freed et al. are only concerned with providing a classic SSL connection between the client and server through an intermediary device.

It is respectfully submitted that the instant amended claimed invention is not taught, disclosed or suggested by Aziz, Gast or Freed et al. taken alone or together. The instant invention is respectfully submitted to be patentably distinct over the art of record. Withdrawal of the rejection of claims 1-19 is respectfully requested. Claims 20-23 are also believed to depend from otherwise allowable claims and define the concurrent connections as one of direct and indirect connections.

Therefore, allowance of claims 1-23 is requested at as early a date as possible. This is intended to be complete response to the Official Action dated 5/12/2008 which with a two month extension and fee herewith fell due on a holiday. This response is believed timely.

Respectfully submitted,

/R. William Graham/

R. William Graham, 33,891

Certificate of Transmission

I hereby certify that this correspondence is being electronically filed with the PTO for group 2137on the date shown below.

/R. William Graham/

Date. Tuesday, October 14, 2008 R. William Graham, 33,891